2014–2018 State Strategic Plan

FOR INFORMATION RESOURCES MANAGEMENT

Texas Department of Information Resources
November 1, 2013

Message from the State CIO

Information technology continues to enable the relationship between Texans and their state government. It is integral to how state agencies deliver services and interact with the public. Information technology enables

- citizens to renew their driver licenses over the Internet and follow elected officials via social media
- state employees to connect to their offices from any secure location allowing for higher productivity
- students to keep abreast of campus activities with their smart phones and receive courses delivered over the Internet
- entrepreneurs to meet state requirements for establishing a business via Texas.gov

This State Strategic Plan for Information Resource Management (SSP) looks at the Top 10 Technology Priorities that will affect state agencies, colleges, and universities for the next five years. While technology is a rapidly changing environment, we believe these priorities provide the greatest opportunities to enhance the relationship between government and citizens in Texas.

State agency business executives and information technology leaders are encouraged to review each priority to determine short- and long-term opportunities for enhanced service delivery. We also encourage you to look for opportunities to collaborate across the state information technology enterprise. While not all priorities are appropriate for all state agencies, each bears monitoring as they represent areas for development at the Texas Department of Information Resources.

Technology in Texas is already enhancing the business of government and providing better services to citizens. State agencies, colleges, and universities have excelled in implementing creative and thoughtful initiatives such as those featured in this plan. While there are challenges ahead, the talented information technology professionals across the state have the dedication and skill to succeed. Through collaboration, and the continued support of legislative and state agency leaders, the potential of technology in state government will continue to be realized.

This plan is the result of research and collaboration with state government IT professionals, business leaders, and members of the SSP Advisory Committee. We appreciate the generous contribution of our state agency partners and stakeholders who participated in shaping this plan. This collaboration not only produced a valuable roadmap for the future of IT, it also plays a critical role in meeting these priorities. The end result will be enhanced services for Texans.

Karen W. Robinson
Executive Director, Texas Department of Information Resources
Chief Information Officer, State of Texas

Contents

ABOUT THIS PLAN

The Information Resources Management Act (Texas Government Code, Sections 2054.091–094) requires the Texas Department of Information Resources to prepare a state strategic plan for information resources management each biennium. The plan identifies technology priorities for state government over the next five years and guides state agencies as they develop their 2014 agency strategic plans. DIR coordinates with the Governor's Office of Budget and Planning and the Legislative Budget Board to issue detailed instructions for the preparation and submission of agency strategic plans.

Note: For the purposes of this report, the term "state agency" is used to indicate a state agency or a state institution of higher education.

The 2014–2018 State Strategic Plan is available on the Department's website at www.dir.texas.gov.

Texas Department of Information Resources • Post Office Box 13564, Austin, TX 78711 • 512-475-4700

Introduction

The State Strategic Plan for Information Resource Management identifies the Top 10 Technology Priorities that will affect technology decisions in Texas government for the next five years. The Texas Department of Information Resources (DIR) developed these priorities over the past year through collaborative measures including

- convening an advisory committee of public and private industry technology professionals
- surveying CEOs, CIOs, and information resource managers (IRMs) in state agencies
- consulting multiple stakeholders and subject-matter experts
- conducting in-depth research and analysis of top technology trends and priorities impacting both government and the private sector around the country

The nature of information technology is one of rapid advancements and constant change, which makes the role of IT in government a balancing act between citizen expectations, innovative options, efficiency measures, and budget constraints. The role of IT in the state's overall ability to deliver quality services to citizens continues to grow. With this growth comes challenging decisions on how to best prioritize agency and statewide investments in technology.

State agencies should consider each of the Top 10 Technology Priorities for its significance to agency operations and service delivery. Given the decentralized nature of IT in Texas government and the diversity of missions, some priorities may not be as relevant to some agencies as others. Each agency must make informed decisions, based on its unique business needs, to determine how these priorities align with its business goals and IT strategic plan.

Because business needs and technology vary by agency, the priorities have not been assigned a numerical ranking at the enterprise level; however, they are presented in three general groups:

- The first three priorities—Security and Privacy, Cloud Services, and Legacy Modernization—are of significant interest to state leadership as illustrated by recent legislative action.
- The next four priorities— Business Continuity, Enterprise Collaboration and Planning, IT Workforce, and Virtualization—are included as technology priorities for the first time as of this strategic planning cycle.
- The final three priorities—Data Management, Mobility, and Network—were identified in previous planning cycles and remain as priorities for Texas government.

Top 10 Technology Priorities

- Security and Privacy
  Develop governance, policies, and guidelines to secure the technology infrastructure, ensure the integrity of online services, and protect the private information collected from citizens and businesses.

- Cloud Services
  Consider and adopt as appropriate, cloud-based software, platform, and infrastructure services to drive cost-effective and efficient operations.

- Legacy Modernization
  Identify existing mission-critical legacy applications and prioritize their replacement or modernization.

- Business Continuity
  Ensure that critical government information technology services continue in the event of a disaster or a disruption of normal operations.

- Enterprise Planning and Collaboration
  Enhance statewide efficiencies through improved planning and collaboration among and within agencies.

- IT Workforce
  Develop and implement strategies to recruit, retain, and manage a fully trained and qualified IT workforce to meet current and future mission objectives.

- Virtualization
  Virtualize existing server and desktop environments to reduce operational costs and improve service delivery.

- Data Management
  Implement sound data management principles to support good business practices, meet regulatory requirements, and reduce costs.

- Mobility
  Support the needs of an increasingly mobile citizen and workforce population.

- Network
  Provide innovative network services to allow agencies to improve efficiency and successfully deliver citizen services.

Security and Privacy

Develop governance, policies, and guidelines to secure technology infrastructure, ensure the integrity of online services, and protect the private information collected from citizens and businesses.

State government transmits, stores, and uses a significant amount of data that must be protected from multiple security threats including loss of confidentiality, integrity, or availability through either malicious or accidental activity. As the steward of personal information for a substantial number of its citizens, the state must maintain the privacy of records that contain personal information.

In Texas, cybersecurity is a shared endeavor with DIR supporting the state enterprise while agencies are responsible for maintaining security within their own organizations. Citizens entrust the state with their personal information, credit card numbers, and other confidential data with the expectation of secure and private transactions. As the state's citizen-facing services continue to move to online service models, it is critical that all state agencies make the safety and security of state information resources a fundamental management responsibility with the highest level of attention and visibility within each organization.

To help maintain the trust citizens place in the state, DIR offers enterprise-level security program services to help state agencies protect the information assets they manage. Enterprise efforts include

- security policies and standards
- statewide network security operations and services
- security risk management
- training and awareness
- technical support services

DIR has additional authority for delivering network security operations and services for state agencies and others. DIR's Network and Security Operations Center (NSOC) is a secure and resilient facility that provides cost-effective network security services to all state agencies and other eligible state entities. The NSOC is a key component in the defense against threats to critical state assets.

Information security policy dictates how government protects personal information from misuse. Privacy policy indicates the information considered private and the manner in which government collects, stores, uses, and disposes of it. While state information security policy is an enterprise partnership between DIR and state agencies, privacy policies are each agency's responsibility and are governed by agency-specific laws and requirements.

Laws related to security and privacy have been enacted over recent legislative sessions:

- 2009 – House Bill 2004 requires state agencies to notify the public in event sensitive personal information is compromised as a result of an information security breach.
- 2011 – Senate Bill 988 creates the Texas Cybersecurity, Education, and Economic Development Council and HB 300 establishes privacy requirements for patient health records.
- 2013 – SB 1134 provides a framework for cybersecurity planning and SB 1597 establishes a formalized reporting system for state agency security planning.

These efforts enhance the significant safeguards, already existing in state government, to secure the vast amounts of personal information collected and maintained by the state.

Planning for Security and Privacy

Attempted cybersecurity attacks are a regular occurrence for state network operations and individual state agency operations. Planning for security and privacy within the scope of infrastructure and applications is a first step in defending against attempted cybersecurity attacks. DIR was given additional responsibilities by the 83rd Texas Legislature (2013) through SB 1134 and SB 1597 to assist with this planning.

- DIR is establishing a framework for cybersecurity to assist state agencies in developing a strategy for cybersecurity risk assessment and mitigation planning.
- In coordination with state agencies and institutions of higher education, DIR has implemented a Rule Review for Texas Administrative Code Chapter 202 – Information Security Standards.
- State agencies are required to submit a biennial cybersecurity plan to DIR, beginning in FY 2014, which addresses vulnerability reports, staff responsibilities, and best practices, risk management, and other measures to protect information from unauthorized access, disclosure, modification, or destruction.
- DIR collaborates with industry partners to strengthen the state's overall security posture by offering security assessments to participating state agencies.

Best Practices

At the NSOC, security operations are co-located and integrated with statewide network management functions. Security services offered through this facility include

- event monitoring, alerting, and analysis
- technical security assessments
- enterprise intrusion prevention
- training and policy support

The Texas Cybersecurity, Education, and Economic Development Council released a report in 2012 that called for improvements to the infrastructure of state cybersecurity operations using existing

resources and partnerships between government, business, and institutions of higher education. The State Cybersecurity Coordinator, appointed by DIR in 2013, will implement recommendations from the Council's report and promote best practices across the enterprise.

The Texas Health Services Authority will issue a report in January 2014 making recommendations on critical issues related to the electronic exchange of protected health information and options to improve patient access to electronic health records.

Cloud Services

Consider and adopt, as appropriate, cloud-based software, platform, and infrastructure services to drive cost-effective and efficient operations.

Cloud computing is a shared group of computing resources—infrastructure, platform, broker, software—accessed through the Internet on a pay-for-use basis. Cloud computing moves resource acquisition from an asset-based model to a service-based model, eliminating the need to own or maintain a particular computing resource. Because cloud computing resources are provided as a service, they are inherently scalable, readily available, and easily deployed. Cloud services provide a more cost-effective and efficient alternative to asset-based resource acquisition.

Although cloud services are relatively new in the public sector, the model has been tested and is sufficiently mature to be adopted for Texas government. With an increasing number of government-specific private cloud offerings, advances in cloud security, and expected economic benefits, state agencies should evaluate their current environments for potential business advantages that can result from moving to the cloud. The 83rd Texas Legislature (2013) passed HB 2422, which encourages state agencies to consider cloud computing when making purchases for a major information resources project.

The benefits of cloud computing are substantial. The ability to rapidly scale to address peak capacity demands, eliminate lengthy procurement cycles, and increase the speed of service delivery are the primary advantages. These benefits can result in cost savings through reduced infrastructure expense and more responsive business processes. However, it is also important to recognize that the complexity of financial models and corresponding cost efficiencies make it difficult to quantify all financial benefits. Some organizations may not see immediate cost savings. The goal and expectation of deploying cloud solutions should focus first on business needs with cost savings as an important secondary benefit.

Planning for Cloud Computing

State agencies should consider the value, available types of service offerings, and technical requirements of the cloud to determine if cloud computing provides the best solution for the business need. Considerations should include

- an evaluation of business needs and technology infrastructure to determine suitability for migrating to a cloud model
- the identification of applications that should be moved to the cloud (depending on agency needs, higher priority should be given to services that have high per-user costs and low utilization rates, are expensive to maintain, require long lead times to upgrade, or that would benefit the most from innovation)
- a determination of the appropriate cloud service model (private, public, community or hybrid) for the applications selected

- a clear understanding of the underlying data classifications for any applications being considered
- an effective contracting and contract monitoring plan
- a clear definition of service level expectations for the service being contemplated
- the security requirements that must be met prior to considering cloud options
- the ability to support business continuity and disaster recovery plans

Best Practices

DIR offers resources to state agencies that have determined cloud computing is a good business decision:

- The state's current shared service offerings for telecommunications and consolidated data centers provide models for developing a successful cloud computing service offering.
- Cloud infrastructure, platform, and broker services are available to state agencies through DIR cooperative contracts.
- Community cloud services are provided through the data center services contract in the state's consolidated data centers.

Legacy Modernization

Identify existing mission-critical legacy applications and prioritize their replacement or modernization.

A legacy application is a computer program that is based on older, less efficient technology. Modernizing legacy applications—whether through replacement or extending compatibility with new systems—can be expensive and complex. However, failure to modernize legacy applications may cause state agencies to be dependent on obsolete technology, which costs more to operate, has fewer benefits, and diminishes capabilities. Within Texas government, 55 percent of state agencies report having at least one mission-critical legacy application.

The maintenance of legacy applications remains a challenge due to limited funding, reduced staff resources, and decreasing vendor support. These challenges limit the ability to enhance or revise legacy systems and create obstacles to retaining technical staff to sustain or upgrade aging systems. State agencies should consider prioritizing budgets toward application modernization for immediate efficiency gains, reduced risks and costs, and improved services.

The 83rd Texas Legislature (2013) passed HB 2738, which directs DIR to conduct a study to identify legacy systems maintained by state agencies. By law the study includes

- an inventory of the systems maintained by state agencies
- the annual cost and availability of resources to maintain the systems
- the security risks related to the use of the systems
- if feasible, a cost estimate for updating the systems
- a plan for assessing and prioritizing modernization projects to update or replace the systems

DIR is actively working with state agency IRMs to comply with the requirements of this legislation and will produce a report and recommendations to the Legislature by October 2014.

The Path to Legacy Modernization

State agencies should address modernization efforts holistically and within the context of the existing technology platform, long-term strategic planning goals, and budget requests. Even though DIR is conducting a statewide study of legacy applications, each state agency should plan modernization efforts and evaluate of its applications portfolio. This process, which focuses on identifying cost, risk, and performance factors, requires a state agency to

- appraise the legacy system
- evaluate the target technology
- define the target architecture
- define the modernization strategy
- reconcile the strategy with stakeholder needs
- estimate the resources required for modernization

For each legacy application slated for review, the agency must determine whether the application should be replaced, migrated, or interfaced to work with modern systems. Factors to consider include

- developing internal criteria for evaluating applications based on current and future business needs
- determining continuing operating, maintenance, and replacement costs
- determining the operational risks and unexpected costs of application failure
- evaluating the use of managed, shared, or cloud services
- avoiding more technical debt on existing applications

Best Practices

Agencies should focus on building quality software when developing new applications. The goal should be to develop an extensible software architecture that grows with business needs. This can be achieved by

- including legacy criteria when evaluating commercial off-the-shelf products
- evaluating cloud services when applicable
- evaluating the availability of industry support for managed services
- scheduling frequent tests during the development phase
- adopting enterprise architecture principles
- promoting open communication between business and technical teams
- refactoring code when appropriate
- increasing interagency collaboration where applicable

Business Continuity

Ensure that critical government information technology services continue in the event of a disaster or a disruption of normal operations.

State government relies on technology to deliver services. The State of Texas must be prepared to ensure critical operations continue in the face of a disaster or the disruption of services. Business continuity planning is crucial to the recovery of technology assets.

A business continuity plan identifies critical functions and the personnel, facilities, and other resources required to deliver those functions. A plan ensures necessary resources will be available when needed.

Texas law requires that state agencies prepare continuity of operations plans. In coordination with the State Office of Risk Management (SORM), state agency business continuity plans must include detailed information for the resumption of essential functions after an interruption of service. State agencies are also required by rule to maintain a written business continuity plan that specifically addresses the information resources required to resume mission-critical functions.

Planning for Business Continuity

SORM provides general planning resources to help state agencies develop and implement a business continuity plan with the following components:

- plan initiation and management
- functional plan development
- awareness and training
- business impact analysis
- employee contact information
- plan maintenance and event response
- emergency response
- public relations and crisis coordination
- coordination with public authorities
- risk analysis

Best Practices

To improve business continuity planning across the enterprise, more than 30 state agencies are joining together to establish the Interagency Continuity Planning Committee. Committee members will collaborate to produce

- a continuity planning crosswalk that combines Texas legislative requirements, rules, federal guidelines, best practices, and other applicable standards
- tools to help identify mission-critical functions and evaluate the impact of threats and hazards

- templates that support the development of plans, procedures, and risk assessments

The templates and documentation developed by the committee will serve as detailed best practices for developing internal business continuity plans. Additionally, state agencies can join DIR's Data Center Services program for business continuity services, or they can leverage infrastructure as a service from cloud providers via DIR cooperative contracts.

Enterprise Planning and Collaboration

Enhance statewide efficiencies through improved planning and collaboration among and within agencies.

Enterprise planning and collaboration provide processes that enable a group of state agencies to work together on technology solutions. While the de-centralized structure of IT operations in Texas gives state agencies relative autonomy over decisions relating to information resources, there are still opportunities for enterprise collaboration and planning.

The 83rd Texas Legislature (2013) formalized in HB 3093 state leadership's desire to maximize collaboration and coordination. The goal of enterprise planning and collaboration is to enable state agencies to better manage expenditures and operate more effectively.

Whether breaking down internal program silos or working with other state agencies to meet the needs of multiple enterprises, collaboration affects the degree to which the state improves its return on IT investments.

Planning for Collaboration

State agencies should take advantage of planning tools offered by statewide entities and consider agency-wide IT management planning and collaboration efforts. By statute, DIR is charged to coordinate and direct the use of information resources technologies. Resources available through DIR include cooperative contracts, the Texas Project Delivery Framework for major IT projects, IRM collaboration forums, accessibility training, and strategic planning and reporting.

Individually, state agencies need to approach collaboration holistically and ensure policies, processes, and strategies are aligned. Examples include

- reviewing and aligning IT governance across all divisions
- using project management to facilitate cross-division collaboration
- maintaining a structure of well-defined and repeatable processes for IT development
- aligning objectives and outcomes with strategic goals
- implementing online collaboration tools
- engaging the executive sponsorship needed

Best Practices

Successful collaborative initiatives include, but are not limited to, the following best practices:

- evaluating the problem to be solved
- identifying shared issues and aligning those issues with solutions
- assigning an individual or group to evaluate ideas (i.e., a CIO networking group)
- conducting a comprehensive analysis, a business case, and ongoing analytics
- establishing a sound governance model, considering cross-jurisdictional governance

- creating new or building upon existing partnerships (i.e., criminal justice and public safety departments or entities with similar missions)
- developing communications strategy to gain stakeholder support
- using IT effectively to create solutions

IT Workforce

Develop and implement strategies to recruit, retain, and manage a fully trained and qualified information technology workforce to meet current and future mission objectives.

Workforce planning is generally discussed in association with human resources strategic planning, not information technology. However, one of IT leadership's greatest challenges is recruiting and retaining a qualified workforce. Skilled professionals are needed to plan, develop, and manage IT solutions. IT staff play a vital role in mission-critical decisions and effective service delivery. IT professionals have a direct impact on an agency's operations and overall success. A strategic focus on building a skilled and efficient IT workforce is essential.

An aging state workforce, competition for skilled workers, and the need to keep pace with innovative technologies are all current realities. Add in generational differences in work methods and expectations, and workforce planning becomes an essential part of IT strategic planning.

Planning for the IT Workforce

IT workforce planning is critical:

- A significant percentage of IT professionals working in state government are currently eligible or will become eligible to retire within the next five years. While not all will opt to retire when eligible, the potential loss of experience-based knowledge requires action.
- Contracted services provide cost-efficient alternatives to long-term employment for short-term needs. In part, agencies save the costs of employment benefits with contract labor.
- There is a relative shortage of qualified technology professionals within the workforce, and competing for them solely on the basis of compensation leaves state agencies at a disadvantage.
- The inherently rapid changes in IT require ongoing training and development of existing staff at a time when state agencies may have restricted training budgets.

Strategic workforce planning is the practice of determining the future skill sets needed, the skills of the current workforce, and how the gap between the two will be closed. IT workforce planning becomes more complex because the rapidly changing nature of technology adds another dimension to consider. The planning process includes determining whether to hire or to contract for needed skills. State agencies may look to a short-term employment strategy for IT workers or to sources for training existing staff in new technologies.

Best Practices

Recruitment and retention strategies are an important element of workforce planning. State agencies should consider possible sources for uniquely trained IT applicants such as veterans, retired

private and public sector IT workers, contractors, and student interns. Other strategies can make state employment more attractive to potential workers:

- Flexible workplace arrangements such as telework, flextime, or compressed work weeks are particularly attractive to a younger generation of workers.
- Detailed job descriptions will give potential employees a better sense of their work day and can highlight the interesting IT projects underway in state government.
- Personalized training, development opportunities, and access to professional credentialing are powerful tools in recruitment and retention.
- Multidisciplinary job training can keep employees engaged, as well as develop a holistic understanding of the organization's functions.
- Team-driven supervision coupled with recognition of individual work contribution is particularly attractive to a younger generation of workers.
- Keeping current with new and emerging technology will help attract and retain technology workers.

Virtualization

Virtualize existing server and desktop environments to reduce operational costs and improve service delivery.

Virtualization is the creation of a logical (rather than physical) instance of an operating system, server, storage device, or network resource. Traditionally, one would procure a server or desktop and install the operating system and applications directly onto the hardware. With virtualization, the operating system and applications are separated from the underlying physical device.

This priority focuses on two areas of virtualization:

- Server Virtualization – Software is used to divide the physical server into multiple virtual environments.
- Desktop Virtualization – The desktop environment resides on a remote server and is served to users on the network.

State agencies can achieve cost savings through virtualization. Virtualization can reduce hardware costs and staffing costs related to hardware replacement, troubleshooting, software installation, and the management of user accounts.

In addition to cost savings, benefits of a virtualized server environment include increased security, flexible disaster recovery and business continuity capabilities, faster provisioning and redeployment, and easier transition to the cloud.

There are different levels of desktop virtualization. In a fully virtualized desktop environment the entire operating system, applications, and data are stored in a data center, giving administrators full access to support each user account. Desktop virtualization also can be partial by moving selected applications or functions to a centralized location, but not replacing the desktop hardware with fully virtualized hardware (i.e., thin or zero clients). Cost can vary greatly based on the approach; desktop virtualization is typically a strategic rather than a tactical decision. State agencies considering desktop virtualization should seek a full understanding of the business value of virtualization and associated costs.

Planning for Virtualization

Over the years, virtualization has gained momentum across state agencies, and trends suggest that it is widely adopted as a viable technology solution. In Texas, most state agencies have a higher ratio of virtualized server instances to physical servers. This suggests that the state is mature in this area.

For desktop virtualization, strategies that make the move more affordable and valuable to the organization include

- taking an enterprise approach to negotiating contracts, which may lead to better pricing and terms with service providers
- creating standardized templates and configurations in the virtualized environments to achieve efficiency gains from an administrative standpoint
- working closely with business owners to determine requirements that are balanced with security and privacy concerns
- considering desktop virtualization as part of legacy application remediation
- comparing outsourcing versus developing the skill sets needed to administer a virtual environment
- developing a strategy to give the agency flexibility to change and evolve the model as needed

Through the Data Center Services (DCS) program, DIR continues to work closely with state agencies to implement a virtualized server environment as a primary solution. As of July 2013, DCS servers were 46 percent virtualized, and DIR expects virtualized servers will increase to about 70 percent in the next few years.

DCS is also planning to develop a set of standardized virtual hosting platforms for DCS agencies' larger remote legacy data centers, providing a remote virtual platform solution consistent with DCS consolidated data centers. The proposed solution will provide a cost-competitive hosting of DCS workloads, rapid scalability, increased robustness, "right size" server requirements, and ease the transition when migrating to the DCS environment.

Best Practices

When state agencies virtualize their data centers, they should consider these best practices from an operational standpoint:

- place an utmost priority on security, disaster recovery, and continuity of operations
- design virtual systems with the limitations of CPU utilization, memory, and disk space in mind
- review all software licensing impacts
- develop a governance structure for deploying new virtual systems and policies for managing duplication and storage
- work with state agency legal and procurement teams to ensure performance measures, service level agreements, and licensing terms are met by vendor partners and products

Data Management

Implement sound data management principles to support good business practices, meet regulatory requirements, and reduce costs.

State agencies continue to produce and accumulate vast quantities of data. The rapid proliferation of data and the legal and operational requirements to retain, manage, and protect data has created significant challenges for business and IT managers. Digital storage of information offers significantly more benefits than paper storage; however, the related management and administrative costs for digital storage are rapidly growing.

Also, new and dynamic forms of electronic data are emerging across government that require retention strategies. These include third-party hosted services such as social networking sites and cloud services; rich media such as images, videos, and podcasts; and data created on mobile devices.

As the amount of data continues to grow, state agencies are faced with questions regarding the *usability* of data:

- How can data be accessed and converted for useful government purposes?
- How can data be shared among state agencies to improve information value and reduce redundant data collection?
- How can data be made more available to the public, who increasingly expect a more open and transparent Texas government?
- How can confidential and sensitive data be identified and protected?

Data management is defined by the Data Management Association as "the development and execution of architectures, policies, practices, and procedures that properly manage the full lifecycle needs of an enterprise." Data management includes categorizing the value and associated risk of managing data as well as the appropriate level of protection required to secure proprietary data.

Texas government must improve its data management practices across the entire data lifecycle from creation to disposition. The following aspects of data management are of particular importance for state agencies:

- Data Identification/Classification
  An important step in data management is to understand the type of data within a state agency and establish a framework for classifying data based on its value, structure, confidentiality, and ability to be shared.
- Data Interoperability/Sharing
  Since state agencies create and collect a vast amount of data across many channels, there is

potential for efficiently sharing data across state agencies with similar missions or interoperable systems.

- Open Data/Transparency
  Increasingly, citizens expect government to enhance transparency by providing non-confidential data for public evaluation and use.

- Big Data/Analytics
  Big data refers to a collection of data that is large and complex making it difficult to process using traditional means. However, it can be mined for correlations and trends not evident in structured data sets. This capability allows users to discover unexpected benefits in well-managed data

- Electronic Records Management
  Electronic records management includes the rules, policies, and guidelines that address the creation, maintenance, retention, and disposition of electronic state records.

Planning for Data Management

A coordinated, enterprise approach to data management promotes the availability of consistent, secure, accurate, timely, and accessible information. Proper data management practices benefit the state by

- eliminating data silos within and across state agencies, allowing data to be shared
- increasing inter-agency and inter-governmental cooperation and trust by improving transparency, data quality, and accountability
- reducing costs through data reuse and standardization
- protecting the privacy of confidential data
- decreasing the likelihood of security incidents due to improper data classification
- ensuring appropriate levels of access
- increasing innovation by allowing third parties to create new uses for datasets
- increasing business intelligence by enabling “big data” analytical methods
- providing support for continuity of operations
- providing support for e-discovery
- ensuring compliance with record management policy

Best Practices

There are a number of current practices in Texas government that support sound data management:

- Texas state agencies are required to develop controls to ensure the confidentiality, integrity, and availability of data.

- Agencies implement internal data governance structures to guide agency-wide data decisions and policies.

- The Texas Legislature recognizes the importance of open data and, through statute, requires state agencies to post high-value data sets in a standard format that allows the public to search, extract, organize, and analyze the information. The Legislature also requires state agencies to develop a Records Management Program and assign a Records Management Officer to administer the program.
- Texas.gov provides a centralized site that offers links to open data posted by state agencies for public use.

Mobility

Support the needs of an increasingly mobile citizen and workforce population.

Mobility describes the ability of employees to perform their duties while away from the traditional office environment. With 56 percent of American adults owning a smart phone and 34 percent owning a tablet computer, the demand for mobile services is growing and will continue to do so. Mobility impacts the relationship citizens have with government and offers opportunities for Texas government to expand its services to citizens and gain greater productivity within its workforce. This ability to connect continues to drive the direction of IT service delivery and customer interaction as citizens expect more self-service applications.

The continually increasing demand for mobile solutions requires government to work toward mobile platforms and frameworks that create a seamless and consistent user experience across devices, services, and applications. Government can optimize websites on mobile browsers, deploy mobile applications for download, and implement text messaging services to improve performance. It is important for state agencies to integrate the demand for mobile solutions into their overall IT strategy. Good mobile solutions look for opportunities to create value and innovation, and many mobile solutions can be easily deployed at little or no cost.

Planning for Mobility Solutions

State agencies need to develop a mobility strategy that aligns with business need and creates value for customers. There are numerous solutions that can be developed internally or procured from the market place, but not all are cost effective or ideal for an agency's unique environment. Some mobile solutions can be easily deployed at minimal cost and others can be complex, expensive, and difficult to maintain. Based on the growing trend of Internet access from mobile devices, state agencies must consider

- optimizing their online services to make information render quickly on various screen sizes and devices
- identifying services and applications that are appropriate for mobile application so employees can work effectively in the field
- building mobile applications around function and value for citizens
- addressing the different needs of employee-facing applications and citizen-facing applications

State agencies also need to look strategically at improving internal operations with the use of mobile devices by employees. Increased mobility provides more flexibility to workers and increases the viability of telework. In addition to mobile solutions, state agencies must develop appropriate policies regarding "bring your own device" which relates to combining business and personal use on a single mobile device. At a minimum this policy should include

- requirements for security and the protection of confidential information
- a documented strategy on cost bearing

- a distinction between smart phones, tablets, and laptops
- the balance of business and personal use during office hours
- expectations of employees during off hours
- criteria for meeting records retention and public information requirements

Best Practices

Government can benefit from mobile strategy best practices in the private sector. Some of these include

- building toward an architecture that is device agnostic and dynamic enough to support various mobile technology users
- designing and deploying applications and functions for mobile devices where appropriate, understanding that not every desktop or web application needs mobility
- making decisions about developing mobile applications based on data
- deploying platforms that are scalable and built with security in mind
- considering the user experience—e.g., students and younger users will expect their devices to interact with services

Network

Provide innovative network infrastructure and services to allow agencies to improve efficiency and successfully deliver citizen services.

A resilient and reliable network infrastructure is the foundation for data and voice communications, which allow state agencies to deliver services to a variety of constituents. Through innovative network services, state agencies can support a flexible workforce, provide project collaboration within and among state agencies, and offer citizen access to government information.

Texas law requires that state agencies use a consolidated shared network of telecommunications services to enhance efficiencies and reduce redundant systems. DIR provides this enterprise solution for voice, data, and video through the Texas Agency Network (TEX-AN) and the Capitol Complex Telephone System (CCTS).

In addition to traditional telephone and data network services, TEX-AN services have evolved in response to the business needs of government. New services such as Voice over Internet Protocol (VoIP), unified communications, mobile and wireless solutions, as well as conferencing and collaboration tools are driving future network operations and services. The emergence of cloud computing and managed services as a viable alternative for applications and storage needs also has driven the expanding and changing network requirements of the state.

Planning for Network Innovation

As with all technological advances, future network innovations must maintain an appropriate balance between adoption of new technologies and the efficient use and sustainability of existing systems. Several business factors drive network innovation:

- Over half of state agencies report an active mobile workforce highlighting the need for secure and reliable mobile and wireless telecommunications services. “Bring your own device” and telework programs increase the importance of mobile service considerations.
- Industry research and publications indicate the emergence of what is termed “The Internet of Things,” or the expectation of ubiquitous Internet use and connectivity among workers and the public, and continued growth of Internet-based solutions.

Working closely with state agencies, DIR implemented new TEX-AN contracts that provide next-generation communication services, sustainable technologies, and flexible service-level agreements to serve a broad range of state agency requirements:

- DIR is exploring solutions that leverage a VoIP platform on the Capitol Complex Telephone System. Pilot projects have proven the reliability and functionality of VoIP as an enhanced

communication solution. DIR is testing *unified communications*, which allow remote workers, field staff, and teleworkers access to voice, voice mail, email, and text messages.

- Upgrading Internet services in the Capitol Complex will lead to greater transmission capacity as the demand for cloud services and more applications increases.
- Beyond the Capitol Complex, the state's Austin metro network is pursuing a renovation that will result in functional benefits for Austin-based state agencies.
- DIR is exploring wireless services as an alternative *last-mile solution*—offering efficiencies at both metropolitan locations and remote offices throughout the state.

Best Practices

To prepare for the transition of communications to digital transmission, state agencies should continue to upgrade internal data networks to ensure continued bandwidth, quality of service, reliability, and security for transmitting video, voice, and data.

As mobile communications services and applications continue to grow, state agencies should prepare operations, policies, and planning to meet the future demands of an increasingly mobile workforce and the current expectations of citizens to interact with government.

Plan Development Process

The approach to a new State Strategic Plan is to build on the previous biennium's plan by updating technology priorities to reflect new trends, continuously engaging stakeholders, and taking a holistic view of the strategic planning life cycle.

The top technology priorities for the SSP were determined through a combination of methods:

- a survey to CEOs and information resource managers (IRMs) at all Texas state agencies, colleges and universities
- the findings of the SSP Advisory Committee
- extensive research across national and state government technology publications
- feedback from IT and business stakeholder groups

SSP Survey

DIR surveyed CEOs and information resources managers (IRMs) for input on current and future technology priorities. The survey assessed the technology priorities from the 2012–16 plan and evaluated eight potential priorities initially considered for this year's plan.

The survey asked respondents whether each existing priority and proposed new priority would be critical to the agency's business strategies in the next biennium. It also asked whether the agency had made progress implementing each technology priority.

The survey ranged on a scale from 1 through 5, in which 5 represented "Strongly Agree," 3 represented "Neutral," and 1 represented "Strongly Disagree." Survey respondents were also given the opportunity to provide additional comments and feedback regarding the technology priorities or other technology areas that were important to their agency. There were 79 respondents to the survey representing small, medium, and large agencies, as well as institutions of higher education. The SSP survey and the results are available on the DIR website.

SSP Advisory Committee

The SSP Advisory Committee members were selected to represent various positions within the technology, public, and private sectors from diverse geographic areas of the state. This group has been instrumental in developing the strategic technology priorities addressed in the plan.

The 18-member committee provided perspective and insight during the planning process. DIR also conducted a series of webinar discussions on specific priorities. Once the top 10 technology priorities were identified and action statements completed, DIR posted the results on its website and solicited feedback from stakeholders.

Glossary

Administrative rules
Rules passed by state agencies that implement relevant sections of state law and are codified in the Texas Administrative Code.

CEO
Chief Executive Officer

CCTS
Capitol Complex Telephone System

E-Discovery
Electronic discovery, a phase in the litigation process through which a party to a lawsuit seeks to obtain information in electronic format that is relevant to its case.

EIR
Electronic and Information Resources

Encryption
A process applied to text messages or other data that alters the information to make it humanly unreadable except by a decryption device or someone who knows how to decrypt it.

GIS
Geographic Information Systems

HB
House Bill

Interoperability
The ability of two or more technologies to exchange information and use the information that has been exchanged.

IP
Internet Protocol

IR
Information Resources

IRM
Information Resources Manager

ISO
Information Security Officer

IT
Information Technology

IVR
Interactive Voice Response

NASCIO
National Association of State Chief Information Officers

NEIM
National Information Exchange Model

NSOC
Network and Security Operations Center

RFO
Request for Offer

RMICC
Records Management Interagency Coordinating Council

SB
Senate Bill

TAC
Texas Administrative Code

Texas.gov
The official website of the State of Texas

TEX-AN
Texas Agency Network